Sub A2

What is claimed is:

1. A data usage controlling apparatus that

(1) reads a type 1 key from a storage unit and

(a) main data,

(b) an encrypted type 2 key produced by encrypting a type 2 key using the type 1 key, and

(c) encrypted condition information produced by encrypting condition information using the type 2 key

from a recording medium,

(2) decrypts the encrypted condition information using the type 2 key, and

(3) controls usage of the read main data based on the condition information,

the data usage controlling apparatus comprising:

first updating means for updating the condition information in accordance with usage of the read main data;

generating means for generating a new type 2 key in accordance with the usage of the read main data;

first encrypting means for encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on the recording medium with the encrypted updated condition information;

second updating means for updating the type 1 key in the storage unit in accordance with the usage of the read main data; and second encrypting means for encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key.

2. A data usage controlling apparatus that

(1) reads a type 1 key from a storage unit and a set including

(a) main data,

(b) an encrypted type 2 key produced by encrypting a type 2 key using the type 1 key, and

(c) encrypted condition information produced by encrypting condition information using the type 2 key

from a recording medium on which n (where n is an integer no less than two) sets of main data, an encrypted type 2 key, and encrypted condition information are recorded,

(2) decrypts the encrypted condition information using the type 2 key, and

(3) controls usage of the read main data based on the condition information,

the data usage controlling apparatus comprising:

generating means for generating a new type 2 key in accordance with usage of the main data;

first encrypting means for encrypting the condition information using the new type 2 key and replacing the

A2

encrypted condition information on the recording medium with the newly encrypted condition information;

decrypting means for decrypting all (n-1) encrypted type 2 keys on the recording medium that are not included in the read set using the type 1 key;

updating means for updating the type 1 key in the storage unit after the decrypting means has decrypted all (n-1) encrypted type 2 keys; and

A2

second encrypting means for encrypting the (n-1) type 2 keys and the new type 2 key using the updated type 1 key and replacing all n encrypted type 2 keys on the recording medium with the newly encrypted type 2 keys.

3. A data usage controlling apparatus in accordance with Claim 2, further comprising:

second updating means for updating the condition information in accordance with usage of the read main data,

wherein the first encrypting means encrypts the updated condition information using the new type 2 key and replaces the encrypted condition information on the recording medium with the encrypted updated condition information.

4. A data usage controlling apparatus in accordance with Claim 3,

wherein the generating means generates a new type 2 key every time a user makes a predetermined number of uses of the main data on the recording medium, and

when the generating means has not generated a new type 2 key, the first encrypting means re-encrypts the updated condition information using a same type 2 key as was used to decrypt the encrypted condition information.

A2

5. A data usage controlling apparatus in accordance with Claim 2,

wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key,

the data usage controlling apparatus further comprising:

obtaining means for obtaining the type 3 encryption key; and

second decrypting means for decrypting the read main data using the obtained type 3 encryption key.

6. A data usage controlling apparatus in accordance with Claim 2,

wherein the main data in each set on the recording medium has been encrypted using a type 3 encryption key that is unique to the data usage controlling apparatus,

the data usage controlling apparatus further comprising:

storing means for storing the type 3 encryption key; and

second decrypting means for decrypting the read main data using the stored type 3 encryption key.

7. A data usage controlling apparatus in accordance with Claim 2,

wherein the updating means updates the type 1 key by performing a predetermined calculation on the read type 1 key.

A2

8. A data usage controlling apparatus in accordance with Claim 2,

wherein the updating means updates the type 1 key by adding one to the read type 1 key.

9. A data usage controlling method that

(1) reads a type 1 key from a storage unit and

(a) main data,

(b) an encrypted type 2 key produced by encrypting a type 2 key using the type 1 key, and

(c) encrypted condition information produced by encrypting condition information using the type 2 key

from a recording medium,

(2) decrypts the encrypted condition information using the type 2 key, and

(3) controls usage of the read main data based on the condition information,

the data usage controlling method comprising the following steps:

updating the condition information in accordance with usage of the main data;

generating a new type 2 key in accordance with the usage of the main data;

A2

encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on the recording medium with the encrypted updated condition information;

updating the type 1 key in accordance with the usage of the main data; and

encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key.

10. A computer-readable recording medium storing a program that

(1) reads

a type 1 key from a storage unit and

(a) main data,

(b) an encrypted type 2 key produced by encrypting a type 2 key using the type 1 key, and

(c) encrypted condition information produced by encrypting condition information using the type 2 key

from a recording medium,

(2) decrypts the encrypted condition information

using the type 2 key, and

(3) controls usage of the read main data based on the condition information,

A2

the program including instructions for executing the following processes:

updating the decrypted condition information in accordance with usage of the main data;

generating a new type 2 key in accordance with usage of the main data;

encrypting the updated condition information using the new type 2 key and replacing the encrypted condition information on the recording medium with the encrypted updated condition information;

updating the type 1 key in accordance with usage of the main data; and

encrypting the new type 2 key using the updated type 1 key and replacing the encrypted type 2 key on the recording medium with the encrypted new type 2 key.